$AF/2137

IPW

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	09/930,654
Filing Date	August 15, 2001
First Named Inventor	Treffers, Menno Anne
Art Unit	2137
Examiner Name	Popham, Jeffrey D.
Attorney Docket Number	93418.000047
Confirmation Number:	1920

ENCLOSURES (check all that apply)

- ☒ Fee Transmittal
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavit/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communications to Group (Appeal Notice, Brief, Reply Brief) w/ Appendix A
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Acknowledgement Postcard
- ☐ Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Michael, J. Didas, 55,112, HARTER, SECREST & EMERY LLP
Signature	
Date	May 10, 2006

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Type or printed name	Melanie L. Lavacca		
Signature	Melanie Lavacca	Date	May 10, 2006

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL For FY 2005

Complete if Known	
Application Number	09/930,654
Filing Date	August 15, 2001
First Named Inventor	Treffers, Menno Anne
Examiner Name	Popham, Jeffrey D.
Art Unit	2137
Attorney Docket No.	93418.000047

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($)$500.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify) _____

☒ Deposit Account Deposit Account Number: 03-3875 Deposit Account Name: Harter, Secrest & Emery LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayments of fee(s)under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
- 20 or HP =		25 =	

HP = highest number of total claims paid for, if greater than 20

Multiple Dependent Claims Fee ($)	Multiple Dependent Claims Fee Paid ($)

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
- 3 or HP =	x	100 =	

HP = highest number of independent claims paid for, if greater than 3

3. APPLICATION SIZE FEE

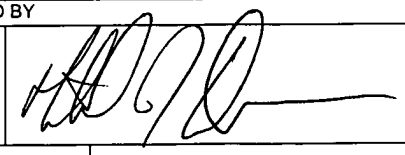
If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listing under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
100 =	0 / 50 =	0 (round **up** to a whole number) x	$250.00 =	$.00

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Appeal Brief	$500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 55,112	Telephone 585-231-1411
Name (Print/Type)	Michael J. Didas	Date	May 10, 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of:
Menno Anne Treffers et al.

US Application No. 09/930,654

Examiner: Popham, Jeffery D.

Confirmation No. 1920

Filed: August 15, 2001.

Group Art Unit: 2137

Attorney Docket No. 93418.000047

For: METHOD AND DEVICE FOR CONTROLLING DISTRIBUTION AND USE OF DIGITAL WORKS

May 10, 2006

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL

Appellants hereby appeal the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims as set forth in the Office Action mailed October 17, 2005, which rejections were upheld in the Advisory Action mailed on March 3, 2006.

A timely Notice of Appeal was filed March 10, 2006.

Real Party-in-Interest

UQE, LLC is the real party-in-interest in this proceeding.

Related Appeals and Interferences

No appeals or interferences are known which will directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

Status of the Claims

Claims 1 through 13 are pending in the application. All of the claims have been finally rejected, and are being appealed herein. Appendix 1 provides a clean, double-spaced copy of the claims on appeal.[1]

Status of Amendments

No amendments were filed in this application subsequent to the final rejection.

Summary of Claimed Subject Matter

The invention relates generally to a method and device for controlling distribution and use of digital works. Throughout, the following discussion, references to the subject application are to the Substitute Specification filed August 7, 2005.

According to one particular aspect of the invention, independent Claim 1 recites a method of controlling distribution and use of a digital work. The method includes an attaching step, a storing step, an updating step, a refusing step, and a changing step. In the attaching step, a usage right information is attached to the digital work DW. The usage right information defines one or more conditions which must be satisfied in order for a usage right of the usage right information to be exercised. (Page 12, lines 3-16.) In the storing step, the digital work and the attached usage right information are stored on a record carrier 10. (Page 12, lines 3-16.) In the updating step, the attached usage right information is updated with every use of the digital work. (Page 14, line 17 – Page 16, line 20.) In the refusing step, use of the digital work is refused if the usage right information indicates that the usage right has been exercised. (Page 20, lines 21-25.) In the changing step, hidden information KLK stored in a hidden channel and used for encrypting or

[1] Applicants note the term "said" erroneously appears in duplicate in the last line of element (a) of claim 1. Applicants will attend to correction of this error upon completion of this Appeal.

verifying the usage right information is changed when the usage right information has changed. (Pages 13, line 24 – Page 14, line 23.)

In another aspect of the invention, independent Claim 11 recites a record carrier for storing a digital work and a usage right information to define one or more conditions that must be satisfied in order for the usage right to be exercised. (Pages 12, lines 3-16.) The record carrier includes a hidden channel not accessible by commercial reproducing devices. (Pages 12, line 17 – Page 13, line 23.) A hidden information is stored in the hidden channel and is used for encrypting or verifying the usage right information. The hidden information is changed when the usage right information has changed. (Page 13, line 24 - Page 14, line 23.)

In a still further aspect of the present invention, independent claim 13 recites a device for controlling distribution use of a digital work includes writing means, updating means, and control means. The writing means writes to the digital work and an attached usage right information defining one or more conditions that must be satisfied in order for the usage right to be exercised on a record carrier 10. (Pages 12, lines 3-16.) The updating means updates the attached usage right information with every use of the digital work. (Page 14, line 17 – Page 16, line 20.) Control means refuses the use of the digital work if the updated usage right information indicates that the usage right has been exercised. (Page 20, lines 21-25.) The updating means changes a hidden information stored in a hidden channel and used for encrypting or verifying the usage right information when the usage right information has changed. (Page 13, line 24 – Page 14, line 23.)

In another embodiment of the invention, dependent claim 2 recites a method according to claim 1, characterized in that the hidden information is a checksum over a data block containing the usage right information.

According to a still further embodiment of the invention, dependent Claim 3 recites a method as claimed in Claim 1 characterized in that the hidden information is a key used for decrypting the usage right information, and the changing step includes randomly changing the key and re-encrypting the usage right information using the changed key when the usage right information has changed. (Page 15, line 20 – Page 16, line 20.)

In yet another aspect of the invention, dependent claim 8 recites the method of claim 1, characterized in that the digital work is an audio track downloaded from the Internet, and the record carrier is a recordable optical disc, a hard disc, a magneto-optic recording device, a magnetic tape, or a memory card. (Page 11, line 24 – Page 12, line 2; Page 19, line 23 – Page 20, line 4.)

In another embodiment of the invention, dependent claim 12 recites the record carrier of claim 11, characterized in that the record carrier is a recordable optical disc, in particular a CD or a DVD. (Page 15, line 20 – Page 16, line 20.]

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1 and 3 - 13 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Published Patent Application No. 2001/0042043 (Shear et al.) in view of United States Patent No. 6,226,618 (Downs et al.) and United States Patent No. 5,892,900 (Ginter et al.).

2. Claim 2 also stands rejected under 35 U.S.C. §103(a), as unpatentable over Shear et al. in view of Downs et al. and Ginter et al., and further in view of United States Patent No. 6,064,751 (Smithie et al).

Argument

The present invention relates to a system and method for controlling distribution and use of digital works. In conventional systems, usage rights are employed to limit usage of music

tracks purchased on the Internet, downloaded to a PC or the like, and stored in scrambled form on a recordable optical disc. For example, usage rights may allow a song contained on an optical disc to be copied and/or played three times, but copying and/or playing the song for a fourth time is prohibited. The usage rights preferably also are stored on the disc, so as to travel with the music tracks.

Of course, for usage rights to effectively limit usage of a musical track, the usage right must be updated each time the track is played. Accordingly, only devices capable of updating the tracks are preferably used. Moreover, it is desirable that a key used to unscramble the content comprising the track is unique to the disc. In this manner, if the content is copied to another disc, the content cannot be unscrambled.

A "replay attack" has become a conventional way to circumvent the above-described security features. In a replay attack, content and associated usage rights contained on a disc are copied onto another memory, e.g., a disc drive. The copy cannot be played when contained on the disc drive, because the key that is unique to the disc is only usable by the disc. However, when the usage right has been exhausted on the disc, i.e., the song has been played the allotted number of times, the copy stored on the disc drive may be re-copied to the original disc. The original information, including the original usage right, is thus restored on the original disc, allowing again for playing the songs the allotted number of times. The original information may be re-stored on the disc in this manner an infinite number of times.

GROUND OF REJECTION 1

Independent Claims 1 and 13, dependent Claims 5-7, 9, 10, 13

The invention of claim 1 remedies the deficiencies of the prior art by, among other features, storing hidden information used for encrypting or verifying usage right information in a

hidden channel on a record carrier, and changing the hidden information when the usage right information has changed.

Regarding the rejection of Claim 1, the Examiner has taken the position that Shear et al., at paragraphs 169-170, teaches attaching usage right information to the digital work, and storing the digital work and the attached usage right information on a record carrier. The Examiner also cites paragraph 251 of that document as teaching refusing the use of the digital work if the usage right information indicates that the usage right has been exercised. Finally, the Examiner cites paragraph 216-220 of Shear et al. for teaching storing a hidden information in a hidden channel used for encrypting or verifying the usage right information. The Examiner indicates, however, that Shear et al. "does not disclose updating the attached usage right information with every use of the digital work and changing the hidden information when the usage right information has changed."

However, the Examiner indicates that Downs et al., at col. 21, ll. 42-63, "discloses updating the attached usage right information with every use of the digital work." According to the Examiner, it would have been obvious to one of ordinary skill in the art to incorporate the content delivery system of Downs et al. into the rights protection system of Shear et al. in order to enforce the usage rights on the original copy and any new secondary copy. The Examiner indicates, however, that Downs et al. does not disclose changing the hidden information when the usage right information has changed.

The Examiner relies upon col. 136, ll. 37-42, of Ginter et al. as teaching this feature. According to the Examiner, it would have been obvious to one of ordinary skill to incorporate the rights protection system of Ginter et al. into the rights protection system of Shear et al. as

modified by Downs et al. "to lessen time during which each key is used, giving an attacker less ciphertext to use in an attempt to obtain the key. (Column 212, lines 43-52)."

According to Applicants' understanding, Shear et al. discloses cryptographic methods, an apparatus, and systems for storage media electronic rights management in enclosed and connected appliances. At paragraphs 169 and 170, cited by the Examiner, a process for creating a secured disk in a distribution process is disclosed. More specifically, that portion of Shear et al. teaches creating a master multimedia DVD disk 100 from digital information received from various peripheral devices. For example, a digital camera 350, which converts light images into digital information 351, includes a secure node 72A to protect the digital information 351 before it leaves the camera 350. The digital information is supplied to a digital image mixer 356, which in turn provides information to DVD ram equipment capable of writing to master disks 100 and/or to disks from which master disks may be created. Moreover, as shown in Figure 3 of Shear et al., digital information 200, metadata 202, and the associated controls 204 are stored on the storage medium. A key block 208 contains one or more cryptographic keys for decrypting the digital information 200 and the metadata 202. The key block 208 may itself be encrypted by hidden keys 210, which hidden keys are stored in a location on the storage medium 100 not normally accessible.

Thus, Shear et al. teaches storing hidden keys for decrypting a key block containing keys for decrypting content on a DVD. That document does not, however, teach or suggest changing, on a record carrier, a hidden information stored in a hidden channel and used for encrypting or verifying usage right information when the usage right information has changed. Specifically, although keys of Shear et al. are hidden on the DVD, the keys are not understood to be hidden

information used for encrypting or verifying usage right information, and they are not changed when the usage right information has changed.

Downs et al. relates to an electronic content delivery system in which the enforcement of content usage conditions 517 is performed by a content usage control layer 505 and user device 109. Specifically, the content 113 is marked with a copy/play code 523 representing an initial copy/play permission. The content 113 is cryptographically scrambled prior to being stored in the end user device 109. A scrambling key is generated for each content item and the key is encrypted and hidden in the end user device 109. Every time the content 113 is accessed for copy or play, the end user device 109 verifies the copy/play code before allowing descrambling of the content 113 and the execution of the play or copy. The end user device 109 also updates the copy/play code in the original copy of the content 113 and on any new secondary copy.

Thus, Downs et al. teaches marking content at a content provider with copy/play code; scrambling the content before transmitting same to an end-user device; generating a scrambling key for each content item; hiding the key, after encrypting, in the end-user device; and upon access to the content, updating copy/play code. However, Downs et al fails to remedy the deficiencies of Shear et al., noted above. In particular, although a scrambling key for decoding content is hidden on an end-user device, that key is not used for encrypting or verifying usage right information. In addition, although Downs et al. contemplates updating a copy/play code when the content is accessed, that document does not contemplate hidden information stored in a hidden channel on a record carrier and used for encrypting or verifying the copy/play code when the copy/play code has changed. Moreover, the contemplated end-user device of Downs et al. is a personal computer or a specialized electronic consumer device, and the end-user device may provide functions such as creating play lists, managing digital content library, displaying

information and image during content playback, and recording to external media devices. Downs et al. does not contemplate a record carrier as the end-user device, and thus Downs et al. is submitted to be inapposite, as applied to the present invention. A record carrier as contemplated in the claims now at issue would receive information from the end-user device of Downs et al. For example, the record carrier of the present invention may comprise the external media device to which the end-user device of Downs et al. has functioning for recording to.

Ginter et al. teaches a virtual distribution environment (VDE) utilizing special purpose tamper resistant Secure Processing Units (SPUs). Permission records 808 govern the use of an object 300, specifying methods or combinations of methods that must be used to access or otherwise use the object or its contents. These permission records 808 may also include key blocks 810 that store decryption keys necessary for accessing the encrypted content stored within the object. Col. 135, ll. 51-58. The permission records 808 and key blocks 810 are frequently distributed electronically, using secure communications techniques, and thus will frequently be stored only on electronic appliances 600 of registered users. Col. 136, ll. 18-26. Permission records 808 and key blocks 810 for each property can be encrypted with a private DES key that is stored only in the secure memory of an SPU 500, making the key blocks unusable on any other user's VDE node. Col. 136, ll. 37-40. In the preferred embodiment, the one or more keys used to encrypt each permission record 808 or other management information record will be changed every time the record is updated. Col. 136, ll. 37-40.

Thus, Ginter et al. teaches, in a secure processing unit, providing permission records and key blocks having keys for accessing content; encrypting the permission records and key blocks with a DES key; and changing the keys used to encrypt the permission records. Ginter et al. fails to remedy the deficiencies of Shear et al. and Downs et al., noted above. Although Ginter may

teach encrypting permission records and key blocks, and changing the keys used to encrypt the permission records, the keys are not hidden information stored on a record carrier in a hidden channel and used for encrypting or verifying usage right information (permission records) when usage right information has changed. Moreover, Ginter et al, like Downs et al., is submitted to be inapposite, as applied to the present invention. Specifically, the secure processing unit is understood to be a device comprising part of a virtual environment, which is distinct from the record carrier featured in the claims at issue.

For the foregoing reasons, Applicants submit that the cited patent documents fail to teach or suggest at least the combination of changing a hidden information stored in a hidden channel and used for encrypting or verifying the usage right information when the usage right information has changed. Moreover, such combination of features would not have been obvious to one of ordinary skill in the art.

Moreover, there is no motivation to combine the references as suggested. The Examiner seems to suggest that motivation is found in Ginter et al. to combine the references. According to the Examiner, it would have been obvious to use the rights protection system of Ginter with the rights protection system of Shear et al, as modified by Downs et al, in order to lessen the time during which each key is used, giving an attacker less ciphertext to use in an attempt to obtain the key. Applicants submit, however, that the rights protection system of Ginter is irrelevant to the present invention. As described in more detail above, the present invention is concerned, for example, with re-encrypting usage rights on a record carrier after a change in the usage rights, to manage encryption keys such that an attacker is unable to overwrite a newer version of the encrypted usage rights with an older version, in an attempt to undo consumption of one or more rights.

Additionally, there is no motivation even to look to Downs et al. or Ginter et al. Shear et al., like the present invention, is directed to record carriers. Shear et al. provides no motivation to look to virtual distribution environments end-user devices to modify keys contained in a hidden channel. The combination proposed by the examiner could only be made with the benefit of Applicants' disclosure.

In sum, when viewed as a whole, the invention of independent claim 1 contemplates a novel method for controlling distribution and use of a digital work contained on a record carrier. To combat a replay attack, hidden information, stored in a hidden channel of a record carrier and used for encrypting or verifying usage right information, is changed when the usage right information has changed. The cited patent documents, whether taken alone or in proper combination, fail to render obvious the invention of claim 1. Applicants also submit that the combination of the cited patent documents is improper, inasmuch as a requisite motivation to combine the documents is absent.

Accordingly, the rejection of claim 1 is not sustainable, and Applicants request withdrawal thereof.

Claims 5-7, 9 and 10 depend from Claim 1 and are submitted to be patentable over the cited patent documents, at least because of this dependency. Applicants request withdrawal of the rejection of these claims.

Independent claim 13 recites a device for controlling distribution and use of a digital work. The device generally corresponds to claim 1, and is believed to be allowable for the same reasons as independent claim 1. Applicants request withdrawal of the rejection of claim 13.

Independent Claim 11

With regard to claim 11, the Examiner merely indicates that claim 11 is an apparatus claim that is broader than method claim 1 and is rejected for the same reasons as claim 1.

Applicants submit that claim 11 is allowable substantially for the same reasons as independent claim 1. More specifically, the combination of Shear et al., Downs et al., and Ginter et al. does not teach or suggest at least a record carrier including a hidden channel not accessible by commercial reproducing devices, with hidden information stored in the hidden channel; the hidden information used for encrypting or verifying the usage right information and being changed when the usage right information has changed.

Moreover, there is no motivation to combine the references in the manner suggested. While Shear et al. may disclose hidden keys stored in a not normally accessible portion of a disk for decrypting content, that published application does not suggest to one of ordinary skill in the art to look to non-disk technologies to alter the hidden keys such that they are 1) used for encrypting or verifying usage right information and/or 2) changed when the usage right information has changed, as in claim 11. Downs et al. and Ginter et al. relate to encryption in end-user devices and secured processing units in virtual environments, respectively. Absent Applicants' disclosure, one of ordinary skill in the art would not look to these non-disk technologies.

Claims 3 and 4

According to the Examiner, Ginter et al. "discloses that the hidden information is a key used for decrypting the usage right information, wherein the changing step includes randomly changing the key and re-encrypting the usage right information using the changed key, when the

usage right information has changed." The Examiner cites column 136, lines 37-59, of that patent for teaching such features.

The cited portion of Ginter et al. makes no mention of randomly changing a key. In fact, the term random is nowhere in that portion.

Applicants further submit that claim 3, which depends from claim 1, also is allowable for the reasons set forth above with respect to claim 1. Withdrawal of the rejection of claim 3 is requested.

Claim 4 depends from claim 3 and is submitted to be patentable over the cited patent documents at least because of this dependency. Applicants request withdrawal of the rejection of this claim.

Claim 8

The Examiner indicates that Claim 8 is rejected because "Shear et al. discloses that the digital work is an audio track downloaded from the Internet, and the record carrier is a recordable optical disc, a hard disc, a magneto-optic recording device, a magnetic tape, or a memory card (Page 12, Paragraph 178)."

Inasmuch as claim 8 further defines the record carrier of claim 1, independent consideration of Claim 8 is hereby requested. Applicants submit that this claim further illustrates that the record carrier is distinct from the end-user device and secured processing unit of Downs et al. and Ginter et al., respectively. For similar reasons as those discussed above with respect to claim 1, one of ordinary skill in the art would not look to Downs et al. and Ginter et al. to modify features of the disk taught by Shear et al, absent Applicants' disclosure.

Claim 12

The Examiner indicates that Claim 12 is rejected because "Shear [et al.] discloses that the record carrier is a recordable optical disc, in particular a CD or a DVD (Page 11, Paragraph 162)."

Inasmuch as Claim 12 further defines the record carrier of Claim 11, independent consideration of Claim 11 is hereby requested. Applicants submit that this claim further illustrates that the record carrier is distinct from the end-user device and secured processing unit of Downs et al. and Ginter et al., respectively. For similar reasons as those discussed above with respect to claim 11, one of ordinary skill in the art would not look to Downs et al. and Ginter et al. to modify features of the disk taught by Shear et al, absent Applicants' disclosure.

GROUND OF REJECTION 2

Claim 2

Claim 2, which depends from claim 1, is separately rejected for the same reasons as claim 1, but further in view of Smithies, which is cited for teaching "a checksum over a data block containing information (Column 13, lines 51-63)."

Smithies et al. is directed to a document and signature data capture system and method. The portion of Smithies et al. referenced by the Examiner is understood to teach that contents of a signature envelope 10, together with a key provided by a client application 2 are checksummed using a technique as is used for checksumming a file. Thus, Smithies et al. teaches checksumming a key.

However, Smithies et al. does not overcome the deficiencies of the combination of Shear et al., Downs et al., and Ginter et al., discussed above with respect to claim 1.

Accordingly, Applicants request withdrawal of the rejection of claim 2.

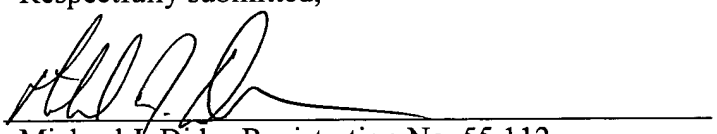
Summary

Even if they are combined, the cited patent documents fail to teach all of the limitations of Applicants' claims. Moreover, there is no motivation to combine the references as suggested.

Conclusion

For the foregoing reasons, Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the rejection by the Examiner and mandate allowance of the claims.

Respectfully submitted,



Michael J. Didas Registration No. 55,112
Customer Number 23387
HARTER, SECREST & EMERY LLP
1600 Bausch & Lomb Place
Rochester, New York 14604
Telephone: 585-231-1411
Fax: 585-232-2152

Appendix I – Claims on Appeal

IN THE CLAIMS:

1. (Previously Presented) A method for controlling distribution and use of a digital work, comprising the steps of:

a) attaching a usage right information to said digital work, said usage right information defining one or more conditions which must be satisfied in order for a usage right of said said usage right information to be exercised;

b) storing said digital work and said attached usage right information on a record carrier;

c) updating said attached usage right information with every use of said digital work; and

d) refusing use of said digital work if said usage right information indicates that the usage right has been exercised;

characterized in that the method further comprises the step of:

e) changing a hidden information stored in a hidden channel and used for encrypting or verifying said usage right information when said usage right information has changed.

2. (Previously Presented) The method according to claim 1, characterized in that said hidden information is a checksum over a data block containing said usage right information.

3. (Previously Presented) The method as claimed in claim 1, characterized in that said hidden information is a key used for decrypting said usage right information, wherein said changing step includes:

randomly changing said key and re-encrypting said usage right information using said changed key, when said usage right information has changed.

4. (Previously Presented) The method as claimed in claim 3, characterized in that the previous key is destroyed after the change of said key.

5. (Previously Presented) The method as claimed in claim 1, characterized in that said hidden channel is arranged to be not accessible by commercial reproducing devices.

6. (Previously Presented) The method as claimed in claim 5, characterized in that said hidden channel is generated by:

- storing said hidden information in deliberate errors which can be corrected again;
- storing said hidden information in merging bits of a runlength-limited code;
- controlling a polarity of predetermined runlength of a predetermined word of a runlength-limited code according to said hidden information;
- storing said hidden information in deliberate errors in a time-base; or
- storing said hidden information in a memory embedded with a disc controller.

7. (Previously Presented) The method as claimed in claim 1, characterized in that said attached usage right information is stored in a table together with a key information used for decrypting said digital work.

8. (Previously Presented) The method as claimed in claim 1, characterized in that said digital work is an audio track downloaded from the Internet, and said record carrier is a recordable optical disc, a hard disc, a magneto-optic recording device, a magnetic tape, or a memory card.

9. (Previously Presented) The method as claimed in claim 1, characterized in that said usage right information comprises a counter information which can be updated when said usage right has been exercised.

10. (Previously Presented) The method as claimed in claim 1, wherein the record carrier has a plurality of tracks, characterized in that each track of said record carrier comprises its own usage right information and hidden information.

11. (Previously Presented) A record carrier for storing a digital work and a usage right information defining one or more conditions which must be satisfied in order for the

usage right to be exercised, characterized in that said record carrier comprises a hidden channel not accessible by commercial reproducing devices, a hidden information (KLK) being stored in the hidden channel, said hidden information being used for encrypting or verifying said usage right information and which is changed when said usage right information has changed.

12. (Previously Presented) The record carrier as claimed in claim 11, characterized in that said record carrier is a recordable optical disc, in particular a CD or a DVD.

13. (Previously Presented) A device for controlling distribution and use of a digital work, comprising:

a) writing means for writing said digital work and an attached usage right information defining one or more conditions which must be satisfied in order for the usage right to be exercised, on a record carrier;

b) updating means for updating said attached usage right information with every use of said digital work; and

c) control means for refusing the use of said digital work if said updated usage right information indicates that the usage right has been exercised

characterized in that

d) said updating means changes a hidden information stored in a hidden channel and used for encrypting or verifying said usage right information, when said usage right information has changed.